AFFIDAVIT OF SPECIAL AGENT DONALD P. MCGRAIL IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT

I, Donald P. McGrail, state:

Introduction and Agent Background

1. I am a Supervisory Special Agent with the United States Secret Service. I have been employed with the Secret Service since 1996. I am currently assigned to the Boston Field Office. My present duties include the investigation of federal offenses including, but not limited to, those involving access device fraud and its related activities, all of which are punishable under the laws of the United States.

2. In preparation for my employment as a Special Agent with the Secret Service, I completed training at the Federal Law Enforcement Training Center in Glynco, Georgia, and the Secret Service James J. Rowley Training Center in Beltsville, Maryland. I hold a B.A. in Legal Studies from the University of Massachusetts at Amherst, and have completed numerous training courses related to constitutional law, criminal investigation, financial crimes, and various fraud schemes.

Purpose of the Affidavit

3. This affidavit is being submitted in support of an application for a criminal complaint charging HELISSON BENAZI DE SOUZA ("BENAZI") with Access Device Fraud, in violation of 18 U.S.C. § 1029(a)(5).

4. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is probable cause for the issuance of the requested complaint and does not set forth all of my knowledge about this matter.

Background

5. Based on my training and experience, I know that fraudsters sometimes obtain blank stored value cards ("gift cards") and use magnetic stripe reader/writers to encode those cards with valid financial account data obtained illegally, *e.g.*, through a data breach or an automatic teller machine ("ATM") skimming operation.[1] Such "cloned cards" constitute counterfeit access devices. *See* 18 U.S.C. § 1029(e)(1)-(2). If the fraudster has the personal identification number ("PIN") associated with the breached account card, he/she can use the cloned card and the stolen PIN to make an unauthorized withdrawal of cash from an ATM.

6. This affidavit concerns BENAZI's use of cloned cards to make unauthorized cash withdrawals from other persons' accounts using ATMs at three banks located in Lynn, Massachusetts, on May 25, 2017.

[1] ATM skimming is described as surreptitiously obtaining the debit card numbers and corresponding PINs of bank customers using an ATM and thereafter making unauthorized withdrawals from those accounts. ATM skimming typically takes place in three stages. In the first stage, the skimmers acquire the account information and PINs of targeted accounts through the use of skimming devices. The skimming devices often consist of two parts, one to record the account information contained in the magnetic stripe on a card, and the other to record the user's PIN. The former is made to look like the legitimate card access slot and does not interfere with the card access functions. The latter is usually a separate pinhole camera device that is discreetly hidden on the ATM or near it in a location from which the customer's input on the ATM keyboard can be observed. Each piece of information is stored on the separate part that recorded it; the information is typically downloaded to a computer and combined. In the second stage, the skimmers create cloned cards by burning the account information obtained by the skimming device onto a blank card, such as a gift card or hotel key card. Then they obtain the PINs for the stolen account by watching the video from the pinhole camera. Often the skimmers will keep track of which PIN belongs to which cloned card by placing on each cloned card a sticker containing the PIN associated with that card. In the third stage, the skimmers go to an ATM and use the cloned cards and the account owner's PIN to withdraw money, typically the maximum withdrawal amount, from the account owner's account.

Probable Cause to Believe That BENAZI Committed Access Device Fraud

7. Shortly after 1 pm on May 25, 2017, Thomas Trusty, a fraud investigator with JPMorgan Chase ("Chase"), contacted dispatch at the Lynn, Massachusetts Police Department. He stated that he was investigating a large number of Chase cards that had been duplicated and compromised. He stated that a significant number of fraudulent cash withdrawals had been made from Chase accounts shortly after 12:00 pm that day from ATMs in Lynn. Mr. Trusty was able to confirm the transactions in nearly real time, and relayed the locations of the ATMs where the cards were being used. Those ATMs were located at three banks in Lynn: (a) Brotherhood Credit Union, 75 Market Street; (b) East Boston Savings Bank, 335 Broadway; and (c) Eastern Bank, 156 Boston Street.

8. Mr. Trusty told Lynn Police Captain Mark O'Toole that the most recent transactions had occurred at Eastern Bank. Captain O'Toole contacted a fraud investigator with Eastern Bank named Thomas Kelleher. Mr. Kelleher viewed surveillance video for the Eastern Bank branch at 156 Boston Street. He told Captain O'Toole that the video showed a man driving a light colored Toyota sedan accessing the drive-up ATM at the bank at approximately 1 pm that day and making multiple transactions.

9. Lynn Police Officer Domingo Polonia proceeded to the Brotherhood Credit Union at 75 Market Street to view surveillance video of the fraudulent ATM transactions.

10. Mr. Trusty again contacted Captain O'Toole, and stated that more fraudulent transactions were being conducted at the Brotherhood Credit Union at 75 Market Street. Captain O'Toole relayed this information, plus the information about the light colored Toyota sedan, to Officer Polonia. Officer Polonia told Captain O'Toole that a silver Toyota Camry with New

Hampshire plates had just left the drive-through of the Brotherhood Credit Union.

11. Captain O'Toole proceeded to the area and entered a parking lot adjacent to the Brotherhood Credit Union. He noticed a lone male in a silver Toyota Camry with the engine running, in the parking lot.

12. Captain O'Toole called for back-up to assist with a stop of the Camry. Two officers in uniform responded. As those officers approached the Camry, the man inside began making sudden movements and reached toward the passenger side of the car. For their safety, the officers removed the man from the Camry and handcuffed him.

13. Officer Polonia arrived at the scene and confirmed that the Camry was the car he had just seen exit the Brotherhood Credit Union drive-through.

14. When asked whether he had a driver's license, the operator said that his license was in his wallet, which was in the car. He gave the officers permission to enter the car to retrieve his wallet. Officers retrieved a wallet but it did not contain a driver's license. It did contain what appeared to be a Brazilian photo identification card that identified the operator as Antony Goulart, d/o/b xx/xx/1982. Because the operator could not produce a valid driver's license, he was taken into custody for Unlicensed Operation of a Motor Vehicle. Lynn police impounded the Camry.

15. The fingerprints obtained during routine booking were entered into the Integrated Automated Fingerprint Identification System, which showed a match for HELISSON BENAZI DE SOUZA, d/o/b xx/xx/1979, of Sao Paolo, Brazil. Captain O'Toole contacted the Boston Field Office of the Secret Service.

16. Lynn Detective Stephen Pohle obtained a search warrant for the Camry from Lynn District Court. When officers executed the warrant, they found, among other things, a Hertz rental agreement in the name of Antony Goulart, $15,180 cash (all in $20 bills), and 203 gift cards. There

were round stickers with numbers on 201 of the gift cards.

17. On May 26, 2017, while in custody at the Lynn Police Station, BENAZI consented to a post-arrest interview. After signing a *Miranda* waiver written in Spanish, he was interviewed by Detective Pohle, Secret Service Special Agent Mario Kirby, and me. Lynn Police Officer Zeke Ortiz translated, using Spanish, which BENAZI indicated he understood. The interview was video- and audio-recorded. BENAZI said that, over the last three days, he and a friend had used gift cards to withdraw a total of approximately $43,000 to $44,000 from ATMs at banks in Massachusetts, including Eastern Bank. BENAZI claimed that the friend had provided the cards. He said the purpose of the stickers on the cards was to write PINs.

18. Agent Kirby and I used a magnetic stripe reader to read the magnetic stripe data on the gift cards found in the Camry.

19. The magnetic stripe data on fifteen of the gift cards matched to debit cards associated with valid Chase accounts from which withdrawals were made between 11:59 am and 1:34 pm on May 25, 2017, at ATMs at the Brotherhood Credit Union, East Boston Savings Bank, Eastern Bank referenced above. The account holders have confirmed that they did not authorize the withdrawals. The following chart summarizes the withdrawals, which totaled $6,880:[2]

[2] BENAZI had sufficient time to drive from East Boston Savings Bank to Eastern Bank (about a 3-minute drive, according to Google maps), and back to East Boston Savings Bank (about a 6-minute drive, according to Google maps), to make the withdrawals shown in the chart.

Time	Bank	Amount withdrawn[3]	Account no.	Account holder
11:59 am	Brotherhood Credit Union	$480	xxxxxxxxxxx5131	A.O.
12:01 pm	Brotherhood Credit Union	$140	xxxxxxxxxxx6865	S.H.
12:04 pm	Brotherhood Credit Union	$480	xxxxxxxxxxx1785	E.S.
12:05 pm	Brotherhood Credit Union	$480	xxxxxxxxxxx3910	D.E.
12:18 pm	Brotherhood Credit Union	$480	xxxxxxxxxxx7048	J.C.
12:24 pm	Brotherhood Credit Union	$480	xxxxxxxxxxx0074	W.D.
12:42 pm	East Boston Savings Bank	$480	xxxxxxxxxxx9402	N.P.
12:43 pm	East Boston Savings Bank	$480	xxxxxxxxxxx7365	W.D.
1:00 pm	East Boston Savings Bank	$460	xxxxxxxxxxx5897	A.N.
1:02 pm	East Boston Savings Bank	$460	xxxxxxxxxxx0277	P.M.
1:08 pm	Eastern Bank	$460	xxxxxxxxxxx4850	C.R.
1:20 pm	East Boston Savings Bank	$500	xxxxxxxxxxx0775	L.S.
1:20 pm	East Boston Savings Bank	$500	xxxxxxxxxxx2670	C.D.
1:33 pm	Eastern Bank	$500	xxxxxxxxxxx8980	S.V.
1:34 pm	Eastern Bank	$500	xxxxxxxxxxx5297	R.M.
TOTAL:		**$6,880**		

CONCLUSION

20. Based on the information described above, all of the withdrawals made by BENAZI discussed above were unauthorized and made use of counterfeit access devices, specifically, cloned debit cards.

[3] These amounts do not include ATM fees that were charged.

21. Based on the information described above, I have probable cause to believe that, on or about May 25, 2017, HELISSON BENAZI DE SOUZA knowingly and with intent to defraud effected transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000, in violation of 18 U.S.C. § 1029(a)(5).

Sworn to under the pains and penalties of perjury.

DONALD P. MCGRAIL
Supervisory Special Agent
U.S. Secret Service

Subscribed and sworn to before me on June 23, 2017.

HON. JENNIFER C. BOAL
Chief United States Magistrate Judge